

January 12, 2024

VIA ECF

The Honorable Mary Kay Vyskocil
United States District Court
Southern District of New York
500 Pearl Street, Room 2230
New York, NY 10007

Re: Joint Amended Letter in *Broidy, et al. v. Global Risk Advisors, et al.*,
Case No. 19-cv-11861

Dear Judge Vyskocil:

Pursuant to the Court's November 29, 2023 Order (ECF 207), the parties respectfully submit this joint letter addressing the topics included in the Court's November 29, 2023 Order.

I. The Nature of the Case, the Principal Claims and Defenses, and the Major Legal and Factual Issues that are Most Important to Resolving the Case

A. Plaintiffs' Statement Concerning the Principal Claims and Major Issues.

This case concerns covert, state-sponsored hacking. Plaintiffs assert that they are victims of a hack-and-smear operation Defendants carried out on behalf of Qatar through the use of computer hacking and surveillance in order to silence Plaintiffs' criticisms of Qatar's support for Hamas and other terrorist groups. Plaintiffs asserts claims under the (i) Stored Communications Act, 18 U.S.C. § 2701, *et seq.*; (ii) Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) and (a)(5); (iii) California Comprehensive Computer Data Access & Fraud Act, Cal. Pen. Code § 502; (iv) Receipt and Possession of Stolen Property, Cal. Pen. Code § 496; (v) common law Intrusion Upon Seclusion; and (vi) Civil Conspiracy. The major legal and factual issues most important to the case involve establishing Defendants' responsibility for the hacking at the heart of this case, given Defendants' extensive measures to conceal the hacking and destroy evidence.

B. Defendants' Statement Concerning the Principal Defenses and Major Issues.

Defendants deny Plaintiffs' allegations and assert that they had no role in the alleged hack-and-smear operation directed at Plaintiffs. While GRA provided Qatar services in connection with Qatar's hosting of the 2022 FIFA World Cup, Defendants were not involved in any way in the alleged hack-and-smear operation, at Qatar's direction or otherwise. Thus, the central issue in this case is whether Plaintiffs can show that Defendants carried out the alleged hack. Discovery will reveal that Plaintiffs cannot adduce evidence to support that contention, nor the false allegation that Defendants destroyed evidence of a hack-and-smear operation.

II. Subject Matter Jurisdiction

A. Plaintiffs' Statement On Subject Matter Jurisdiction and Venue

The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a), because Plaintiffs are Florida and California citizens whereas Defendants are not and the amount in

Honorable Mary Kay Vyskocil
January 12, 2024
Page | 2

controversy far exceeds \$75,000. The Court also has federal question jurisdiction (28 U.S.C. § 1331), because the action arises under U.S. laws and supplemental jurisdiction (28 U.S.C. § 1367(a)) over Plaintiffs' state law claims, because they are part of the same case or controversy. Venue is proper under 28 U.S.C. § 1391(b)(2) and (3) because a substantial part of the events giving rise to the claims occurred in the district, and at least one Defendant resides here.

B. Defendants' Statement On Subject Matter Jurisdiction and Venue

Defendants do not dispute the basis of diversity jurisdiction with respect to the places of incorporation or citizenship of the Defendants, but reserve the right to dispute jurisdiction as to Plaintiffs' citizenship, the amount in controversy, or venue, as well as the grounds for supplemental jurisdiction, based on discovery and any other relevant developments in this action.

III. Motions and Applications

A. Joint Statement on Motions and Applications

Plaintiffs filed their Complaint on December 27, 2019 (ECF 1) and Defendants moved to dismiss on June 12, 2020 (ECF 45). On June 26, 2020, while Defendants' motion to dismiss was pending, Plaintiffs filed an Amended Complaint (ECF 57). Defendants moved to dismiss on August 10, 2020 (ECF 72), which the Court granted on March 31, 2021 (ECF 89). Plaintiffs then moved for leave to file a Second Amended Complaint ("SAC") on June 1, 2021 (ECF 95), which motion the Court granted on February 28, 2022 (ECF 114). Plaintiffs filed their SAC on March 1, 2022 (ECF 116), and Defendants moved to dismiss on May 3, 2022 (ECF 123). On September 26, 2023, the Court granted in part and denied in part Defendants' motion. (ECF 200.) On October 12, Defendants answered the SAC, and in accordance with the Court's order (ECF 203), certain paragraphs were redacted for government review (ECF 204). On November 22, following such review, Defendants filed an updated answer. (ECF 206.) Plaintiffs sought sanctions against Defendants' former counsel Gibson, Dunn & Crutcher LLP on February 23, 2023 (ECF 162), which the Court denied on November 15 (ECF 205).

B. Plaintiffs' Additional Statement on Motions and Applications

Plaintiffs respectfully intend to make the applications set forth in Part IV.B. Further, Plaintiffs need to confer further with the confidential witnesses referred to in the SAC on appropriate protections to safeguard the disclosure of their identities given their view of the threat to their lives and livelihood public disclosure poses. Plaintiffs will then seek to reach an agreement on such protections with defendants. In the absence of an agreement, Plaintiffs may seek relief from the Court to restrict, limit, and/or delay disclosure of their identities.

C. Defendants' Additional Statement on Motions and Applications

For the reasons set forth in Section IV below, Defendants oppose Plaintiffs' anticipated applications and also address Plaintiffs' statement regarding confidential witnesses.

Honorable Mary Kay Vyskocil
 January 12, 2024
 Page | 3

IV. Discovery

Discovery in this action was stayed on June 3, 2020, pending the Court's resolution of the defendants' motion to dismiss. (ECF 44.) On November 29, 2023, after denying Defendants' motion to dismiss the SAC in part, this Court ordered the parties to "commence discovery, if not already commenced." (ECF 207.) To date, the parties have not exchanged any discovery, but anticipate discovery on the topics set forth below in parts B and C.

A. Plaintiffs' Proposed Discovery Schedule, Anticipated Discovery, and Expected Applications to the Court.

Due to the unique circumstances and complexities of this case, as set forth further herein, plaintiffs propose the following departures from this Court's standard practice of the Federal Rules of Civil Procedure: (1) that fact discovery be completed by September 13, 2024, which is 238 days from the January 19, 2024 pre-trial conference; (2) that plaintiffs be permitted 20 fact depositions without further leave of Court; and (3) that plaintiffs be permitted to file a motion to amend the pleadings and to join additional parties until 14 days after the close of discovery.

This case concerns covert, state-sponsored hacking carried out by a large number of actors conspiring together, and requires plaintiffs to uncover conduct and entities that sophisticated hackers have taken great pain to conceal. Accordingly, as illustrated by the following examples, discovery in this case necessarily will be complex and time-consuming.

First, GRA hid its hacking behind multiple virtual private networks ("VPNs") or virtual private servers ("VPSs") owned by third parties based in the U.S., including Micfo LLC and InstaVPS, a standard practice of bad actors seeking to penetrate closed systems. Certain IP addresses were leased to companies that appear to be intermediaries and that, in turn, provided IP addresses to act as VPNs or VPSs used by others. Similarly, GRA distributed stolen emails to the media via (among other means) an anonymous email address, LA.Confidential@mail.com.

Plaintiffs thus expect to issue successive discovery requests to trace the transactions to the end users, including GRA or its co-conspirators. This will likely involve international discovery, as one of the frequently-used VPN providers leased the IPs at issue to a customer in Hong Kong. We expect this will be an iterative process, because we need to work through the layers of obfuscation the attackers intentionally built into their scheme. Issuing discovery in this manner—discovery that is itself aimed at identifying "persons who know of any discoverable matter"—is "deeply entrenched in practice" and is critical in a case like this one, involving sophisticated and concealed wrongdoing. *See* Fed. R. Civ. P. 26, advisory committee's notes to 2015 amendments; *see also* 8A Charles Alan Wright, et al., *Federal Practice & Procedure* § 2046 (3d ed. 2010) ("Often use of one discovery device will lead naturally to use of another.")¹

¹ Defendants cannot dispute that tracing IP addresses and VPN connections from an address used in the hack to the originating address will identify the source of the hack. Defendants' characterization of seeking this information as a "fishing expedition" is unfounded and their attempt to quash basic corroborating evidence is telling.

Honorable Mary Kay Vyskocil
 January 12, 2024
 Page | 4

Second, subpoenas to telephone companies will reconfirm whom the conspirators were calling at relevant times, and assist in uncovering who else (wittingly or not) aided the scheme or has relevant knowledge. Similar discovery was allowed in the related action, *BCM et al. v. Muzin et al.*, 1:19-CV-00150-DLF (D.D.C. Jan. 24, 2019) (the “D.C. Action”).²

Third, in plaintiffs’ experience in the D.C. Action, third-parties involved in the conspiracy have mounted stiff resistance to discovery, funded by Qatar. Plaintiffs reasonably expect the same resistance from other members of the same conspiracy.

Fourth, plaintiffs anticipate requiring, and intend to seek, discovery on a number of relevant subjects, including: (1) defendants’ work for, and payments from, Qatar; (2) defendants’ involvement in GlobalLeaks and prior, similar hacks; (3) investigation of GRA/Qrypt and/or Chalker by law enforcement; (4) computer/network activity logs and data, as well as physical activity logs and data, from dates of hack; (4) documents and communications concerning: (i) plaintiffs/Mowbray/Rosenzweig, Otaiba; (ii) defendants in the D.C. action; (iii) the dissemination of hacked documents; (iv) policies on law enforcement, hacking, privacy, document deletion or retention; (v) communications or meetings between any defendant and any Qatari official and/or agent; and (5) any other topics relevant to the claims or defenses.

Number of Fact Depositions: Plaintiffs should be permitted to take 20 fact depositions, 10 more than permitted to be taken per side without leave of court pursuant to Fed. R. Civ. P. 30(a)(2)(A)(i). At least 20 depositions will be required given the unique complexities discussed above, as well as the number of parties and non-parties with relevant information, including the ten current and former defendants, the three defendants and other third parties in the D.C. Action who were involved in disseminating plaintiffs’ hacked files, and other members of the conspiracy at issue. Given the allegations concerning defendants’ efforts to conceal the hack, including destroying evidence, plaintiffs believe additional depositions are necessary.

Deadline to Amend: This case presents exceptional circumstances warranting motions to amend and to join additional parties to be filed until 14 days after the close of discovery. As alleged in the complaint, defendants have taken great pains to conceal their conduct in furtherance of the conspiracy, as well as the identity of co-conspirators. (*See, e.g.*, SAC ¶ 2.) Plaintiffs therefore expect discovery to unearth additional causes of action, and individuals and entities involved in the conspiracy, that they should be allowed to add to the pleadings.

B. Defendants’ Proposed Discovery Schedule, Anticipated Discovery, and Expected Applications to the Court

Defendants’ Proposed Discovery Schedule. Discovery should proceed on the Court’s standard discovery schedule, including 120 days for fact discovery.

First, Plaintiffs’ proposed discovery amounts to a blatant fishing expedition. Discovery

² Plaintiffs are willing to meet and confer concerning subpoenas issued to obtain records for phone numbers registered in defendants’ names or otherwise associated with defendants that are purportedly used by relatives.

Honorable Mary Kay Vyskocil
 January 12, 2024
 Page | 5

must be “proportional to the needs of the case” and tailored to addressing the issues in dispute. *See* Fed. R. Civ. P. 26(b)(1). Plaintiffs intend to issue “successive discovery requests,” allegedly to trace IP and VPN transactions, based on their speculations and hope to find *something* to pin the hack on Defendants. While Plaintiffs make sweeping allegations that “GRA hid its hacking” behind VPN connections, they present no objective facts to the Court supporting that assertion. Before Plaintiffs are permitted to embark on their iterative and worldwide discovery and prolong discovery for months, the Court must put them to the test—what do Plaintiffs know about these alleged IP and VPN addresses, and does *any* of that connect Plaintiffs’ proposed search into a purported web of international internet connections to Defendants.

Second, Plaintiffs’ proposed discovery into telephone records is another veritable witch hunt. Before the Court stayed discovery, Plaintiffs served 20 subpoenas on 20 telecoms seeking three and a half years’ worth of extensive information related to 178 telephone numbers. Those telephone numbers include, for example, those of Mr. Chalker’s teenage son and wife, and of a college intern who worked at GRA for one semester.³ Insofar as Plaintiffs’ want this discovery to “reconfirm whom the conspirators were calling,” they do not need to conduct duplicative discovery into what they already know. Nor can they burden the Court and Defendants with prolonged discovery so that they can attempt to identify other parties to sue.

Third, Defendants are also concerned by the breadth of Plaintiffs’ descriptions of the subjects of discovery they intend to seek. While Defendants agree that discovery sufficient to establish the nature, scope and duration of the services GRA provided to Qatar is relevant, absent any evidence that GRA participated in hacking Plaintiffs’ computers, the details of Defendants’ business relationships and services unrelated to an alleged hack operation should not be freely available to Plaintiffs.

Finally, Plaintiffs claim that, based on their experience in the related D.C. Action, third parties “have mounted stiff resistance to discovery.” It is premature to extend discovery based on “resistance” unidentified third parties *might* put up in this case. Moreover, it is our understanding that it is Plaintiffs who have produced virtually nothing in the D.C. Action well over a year into discovery. As to party discovery, Defendants are not aware at this time of any reason why that discovery should take twice the Court’s standard period for fact discovery.

Number of Fact Depositions. Plaintiffs’ application to take 20 depositions is premature, excessive and disproportionate to the needs of this case. First, there are only three remaining individual Defendants in this case. Second, Plaintiffs point to the “three defendants” in the D.C. Action. Plaintiffs presumably have or will be obtaining party discovery in the D.C. Action from the defendants in that case, and can then determine whether those defendants need to be deposed. Third, Plaintiffs point to unidentified “third parties” and “other members of the conspiracy.” Those vague references are insufficient to warrant a preemptive doubling of the number of

³ During the December 19, 2023 Rule 26(f) Conference, Defendants inquired from Plaintiffs regarding the status of these 20 subpoenas. Once Plaintiffs provide that update, Defendants reserve the right to object to those subpoenas at least insofar as they encroach on privacy and potentially privilege concerns.

Honorable Mary Kay Vyskocil
January 12, 2024
Page | 6

depositions available to them.

Further Amendments of the Complaint and Joinder of Parties. Under the Court's standard civil case management schedule, "[a]bsent exceptional circumstances," any motion to amend the complaint or join additional parties must be filed within "thirty (30) days from the Initial Pretrial Conference or filing of the Proposed Case Management Plan." Defendants oppose Plaintiffs' anticipated application to extend that time. Plaintiffs have already had three bites of the apple, and should not be permitted to further prolong this litigation. This is Plaintiffs' fourth case in a line of "litigations . . . against Qatar and its alleged agents for the hacking[.]" (ECF 200 at 4.) As noted above, Plaintiffs have had the benefit of a full discovery period in the D.C. Action with respect to the same exact alleged conspiracy.

Plaintiffs' Potential Protective Order. To date, Plaintiffs have not conferred with Defendants on the issue of seeking a protective order in connection with their anonymous witnesses, including the Anonymous Declarant, who submitted a declaration in support of Plaintiffs' SAC. Plaintiffs have now informed Defendants that they intend to rely on these witnesses for trial. Plaintiffs survived a motion to dismiss relying on the Anonymous Declarant, and discovery from this declarant and other unnamed sources referred to in Plaintiffs' complaint is crucial because Plaintiffs intend to rely on those witnesses at trial. This matter must be resolved forthwith. Defendants are available for a meet and confer, and submit that in the event the parties cannot resolve this issue, it must be briefed promptly. Plaintiffs' allegations that their witnesses might need protection from Defendants are hyperbolic and entirely unsubstantiated.

Discovery Defendants Intend to Take. Defendants intend to seek discovery principally into the alleged evidence or lack of evidence supporting Plaintiffs' central allegation that Defendants were involved in the alleged hack-and-smear operation, including without limitation, discovery into any alleged forensic evidence that Plaintiffs claim to have and alleged evidence from the purported "GRA Whistleblower" and any other anonymous witnesses referenced in the SAC, and Defendants' alleged efforts to coordinate with any alleged co-conspirator to disseminate the hacked materials to the press. Defendants also anticipate seeking discovery into the related issue of Plaintiffs' motives and incentives in bringing and maintaining this lawsuit, and Plaintiffs' alleged damages.

V. Settlement Discussions

Pursuant to the Court's order (ECF 207), the parties held a settlement conference on December 13, 2023, which was unsuccessful. At present, the parties do not believe a settlement conference would be productive.

Honorable Mary Kay Vyskocil
January 12, 2024
Page | 7

Respectfully submitted,

/s/ Paul J. Burgo

Daniel R. Benson

Paul J. Burgo

Kasowitz Benson Torres LLP

Counsel for Plaintiffs

/s/ Marc A. Weinstein

Marc A. Weinstein

Amina Hassan

Kiran Rosenkilde

Hughes Hubbard & Reed LLP

Counsel for Defendants